

Designing Data Architectures that InfoSec will actually approve



Craig Porteous

Principal Consultant



<https://craigporteous.com>



[@cporteous](https://twitter.com/cporteous)



<https://github.com/cporteous>



[@ADVANCINGANALYTICS](https://www.instagram.com/advancinganalytics)



[@ADVANALYTICSUK](https://twitter.com/advanalyticsuk)



[/ADVANCING ANALYTICS](https://www.youtube.com/advancinganalytics)

Designing Data Architectures that InfoSec will actually approve



Craig Porteous

Principal Consultant



<https://craigporteous.com>



[@cporteous](https://twitter.com/cporteous)



<https://github.com/cporteous>



[@ADVANCINGANALYTICS](https://www.instagram.com/advancinganalytics)



[@ADVANALYTICSUK](https://twitter.com/advanalyticsuk)



[/ADVANCING ANALYTICS](https://www.youtube.com/advancinganalytics)



twoday
capacity

ITPA
CONSULTING



Premium Sponsors

Standard Sponsors

TIME **X** TENDER

[stoltze][it]

ORANGEMAN

 **exmon**

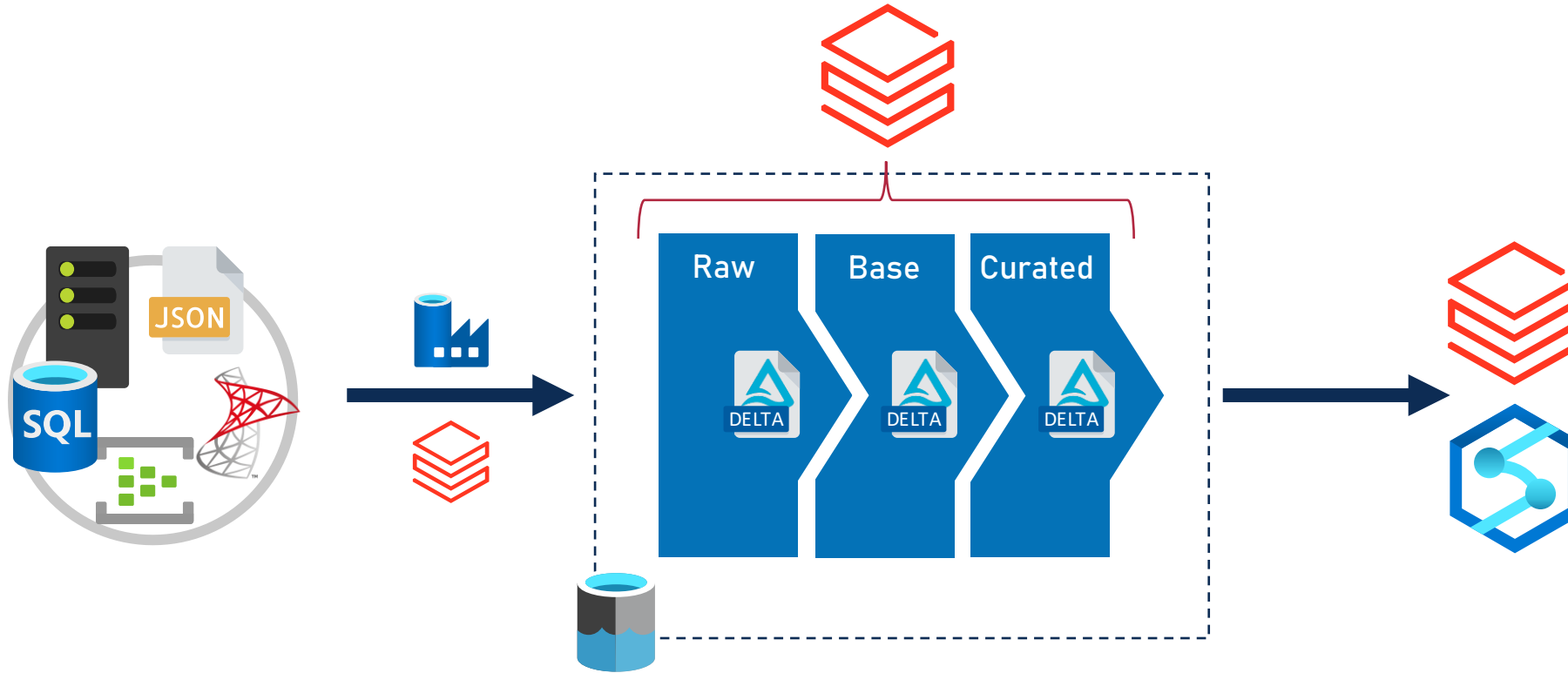

KPMG

Fellowwind

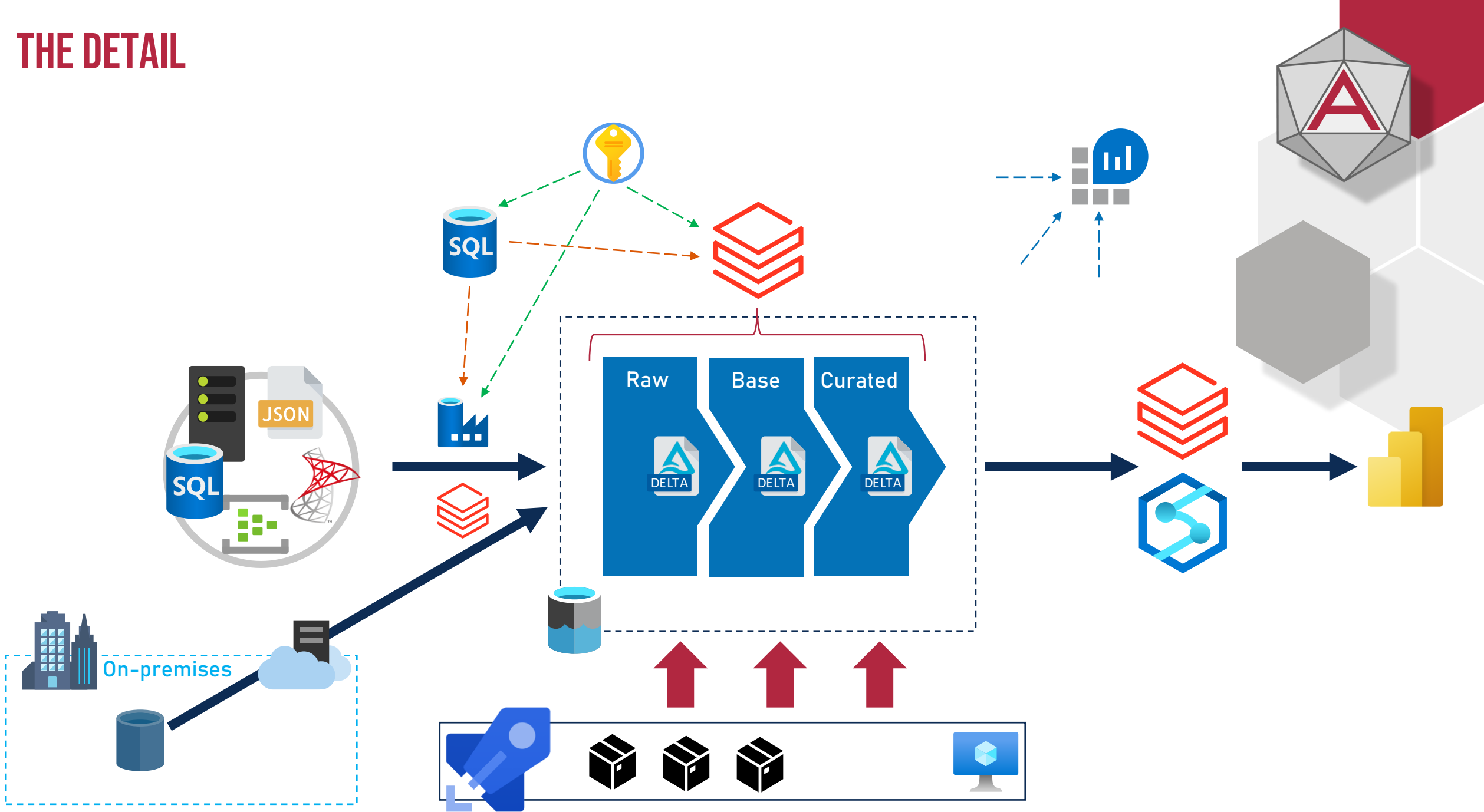


Raffle Prizes

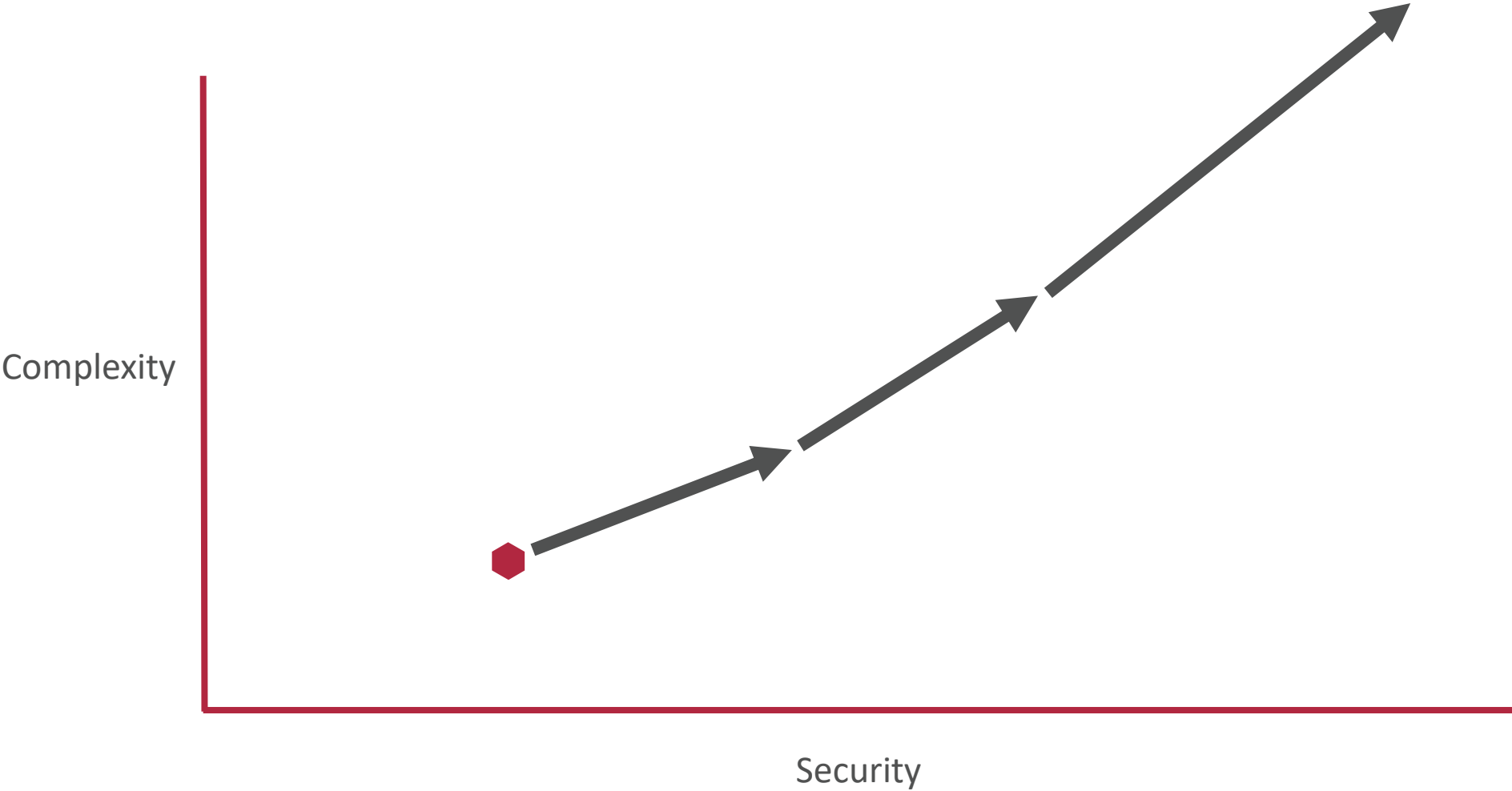
THE DATA PLATFORM



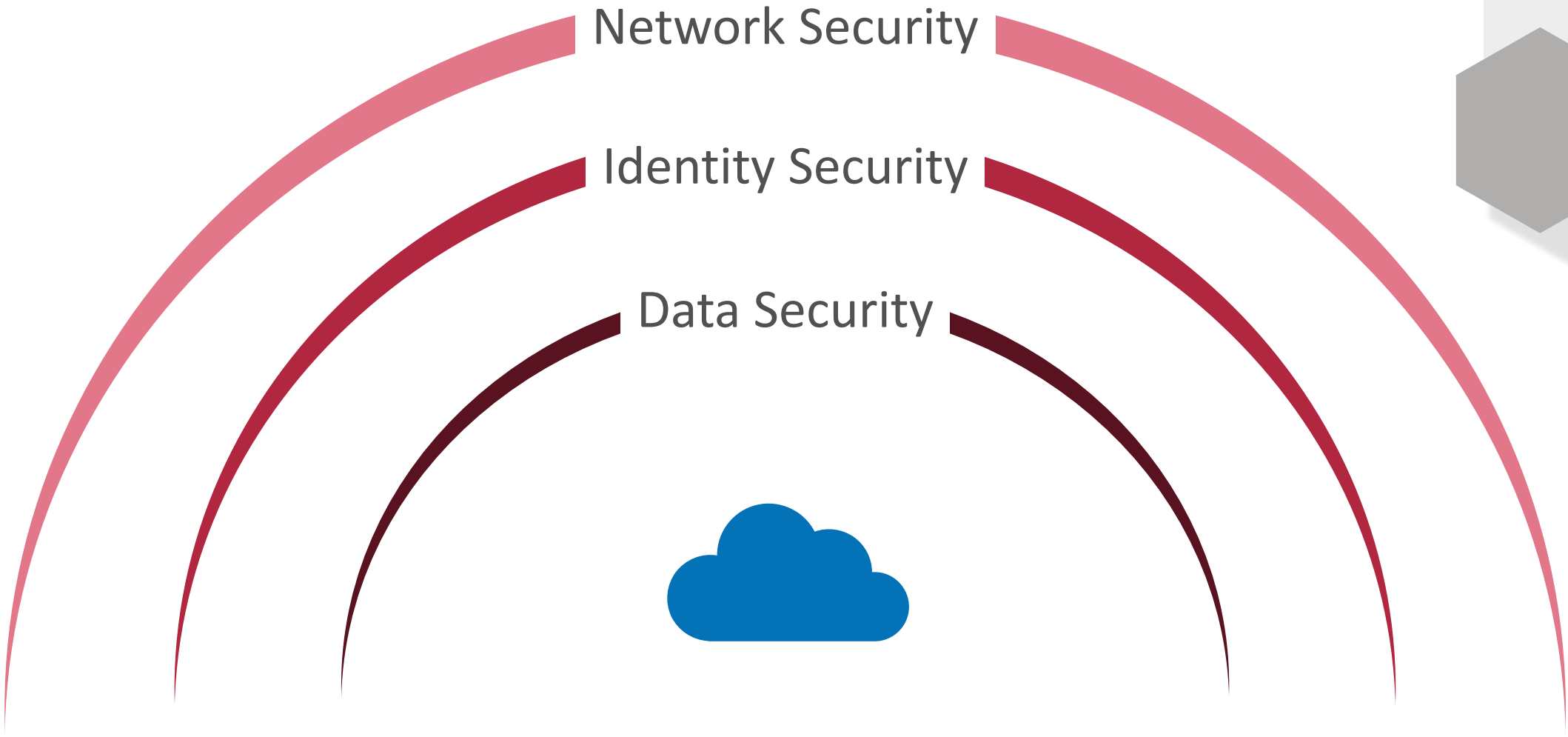
THE DETAIL



WHAT'S THE IMPACT



DEFENCE IN DEPTH

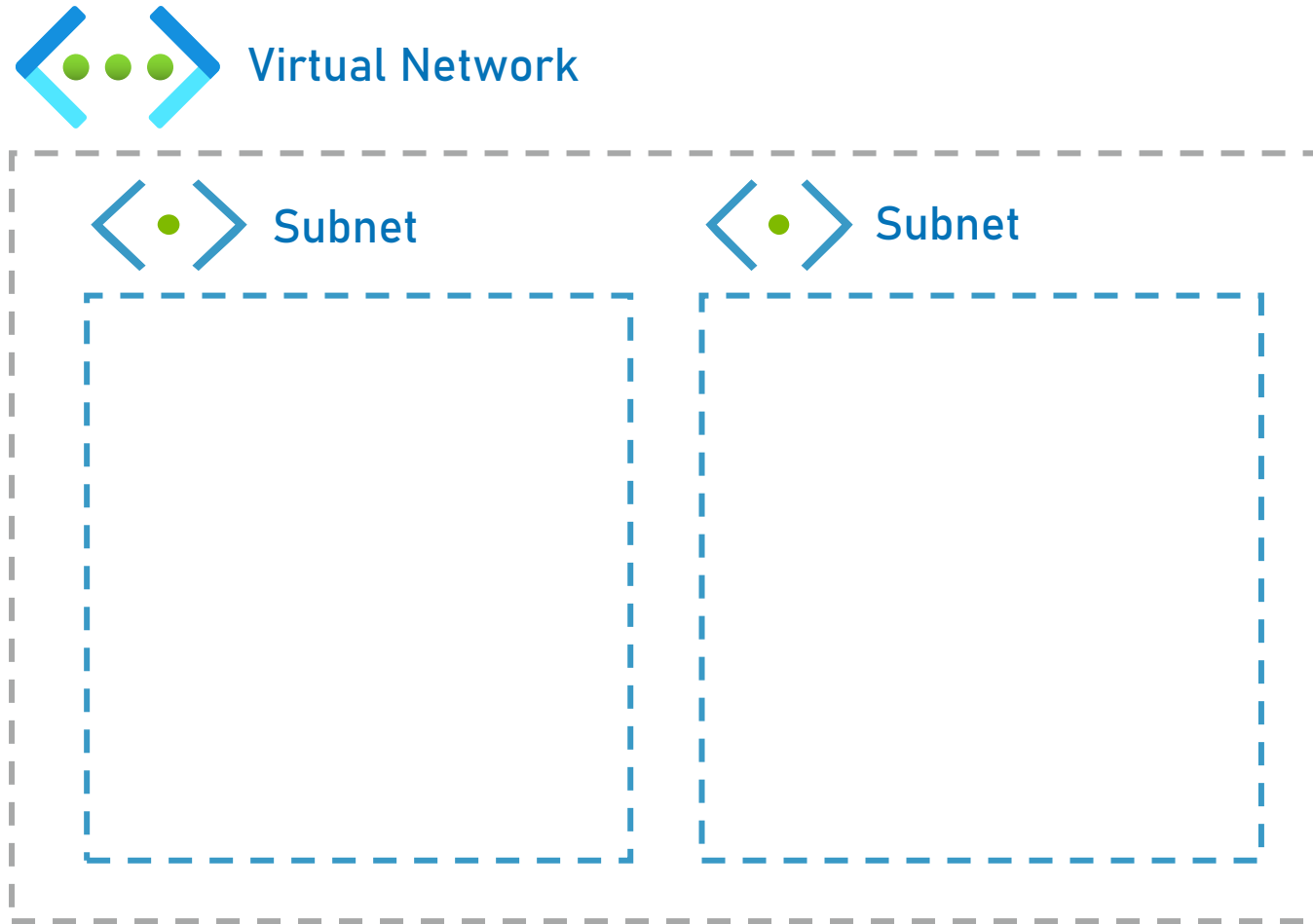




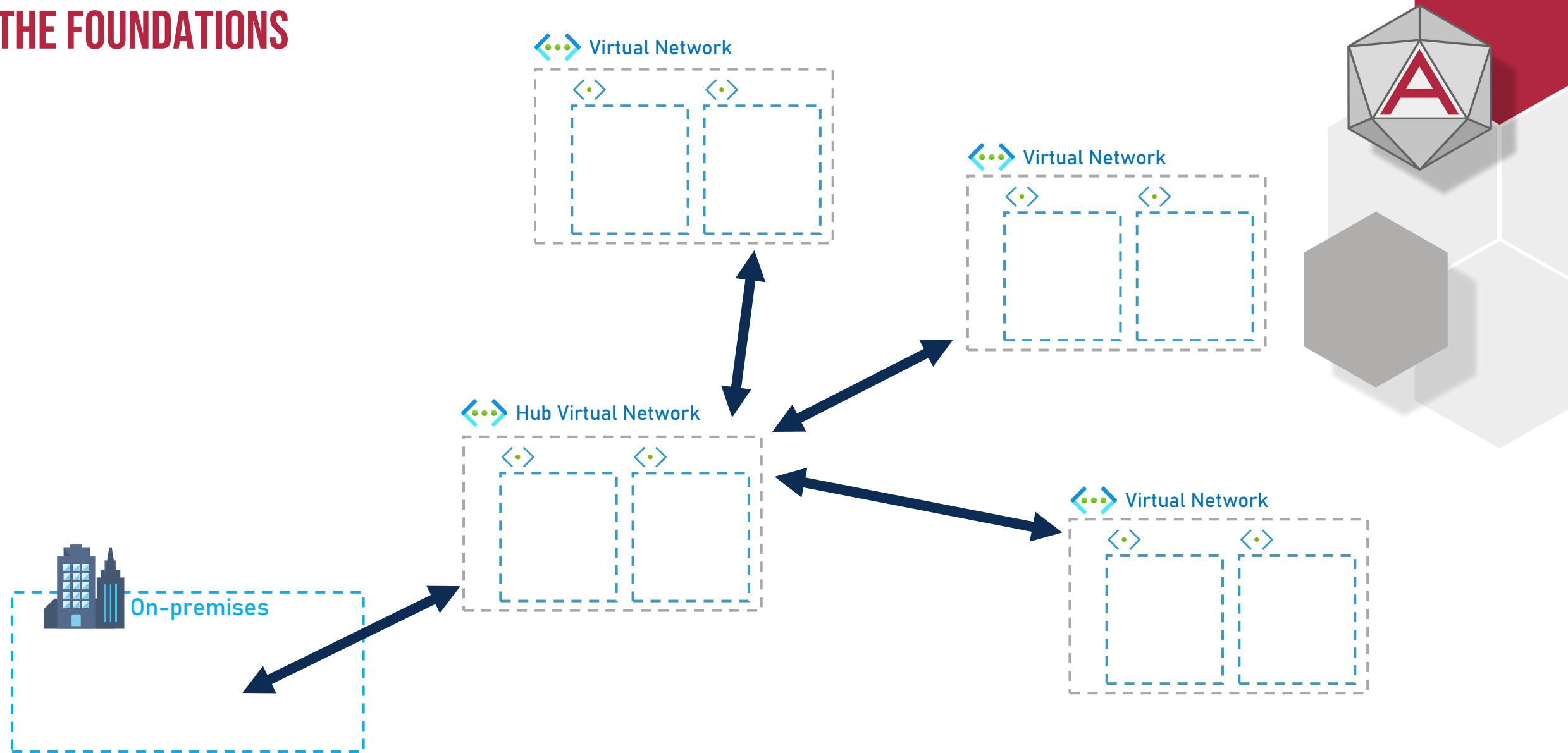
www.advancinganalytics.co.uk

NETWORK SECURITY

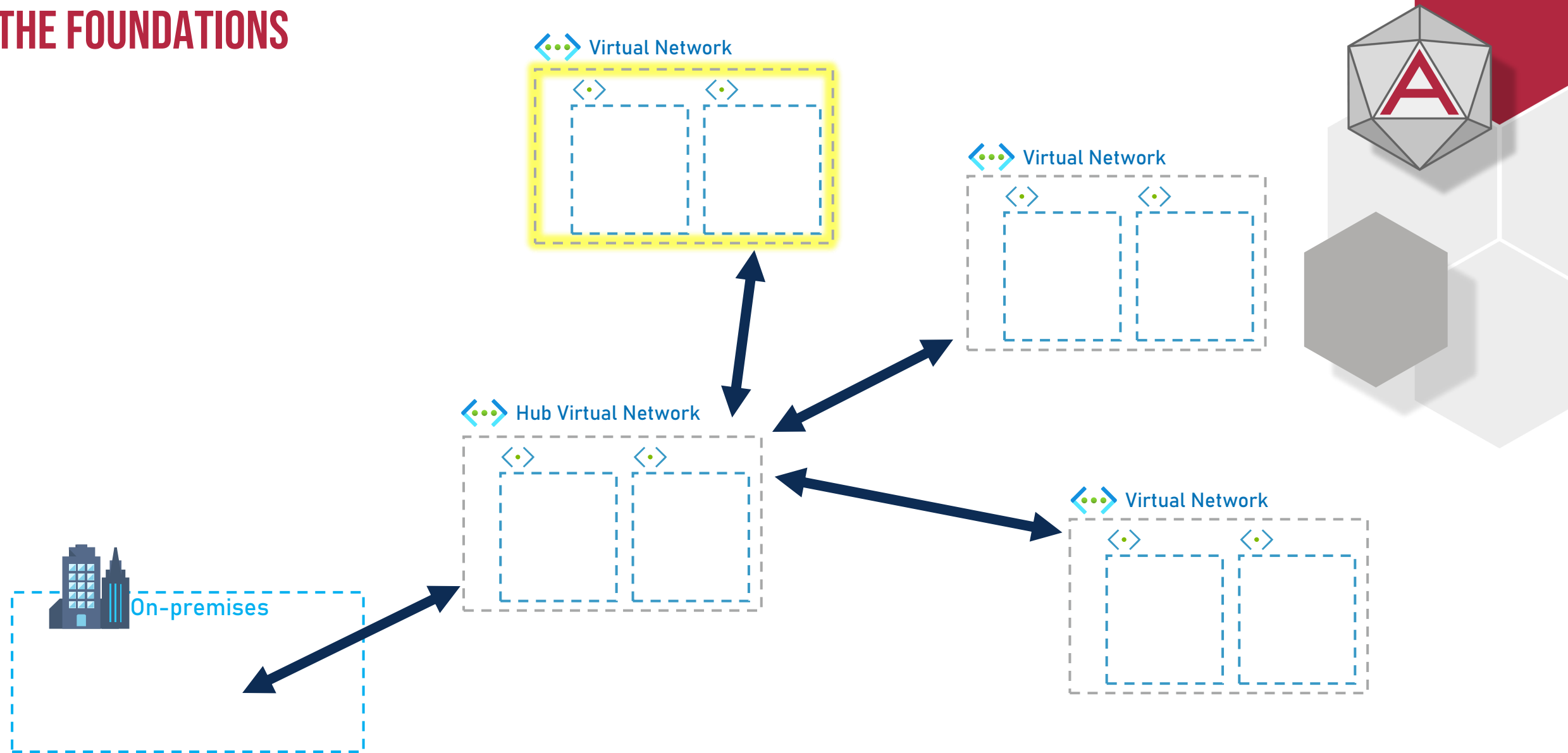
THE FOUNDATIONS



THE FOUNDATIONS



THE FOUNDATIONS



PRIVATE ENDPOINTS



 Virtual Network

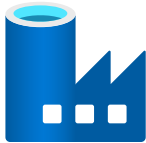
 Subnet

10.X.X.X

 Private Link

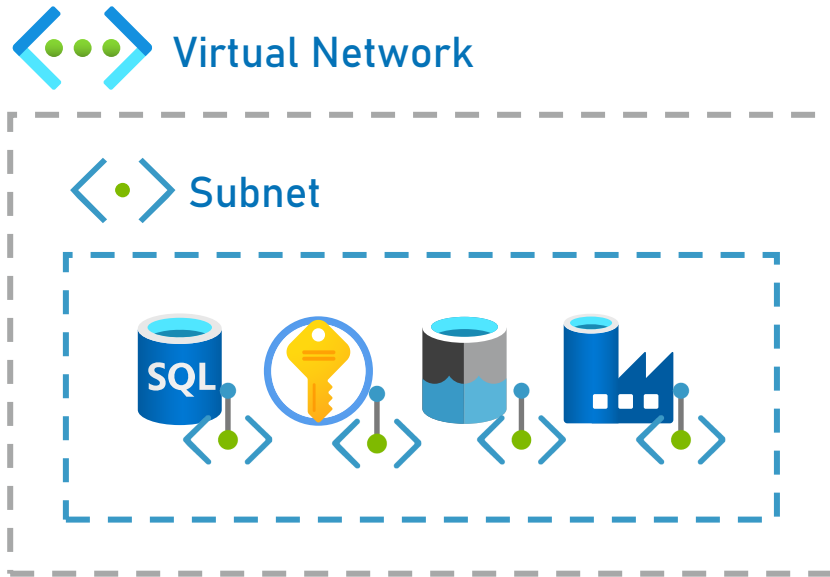


Azure

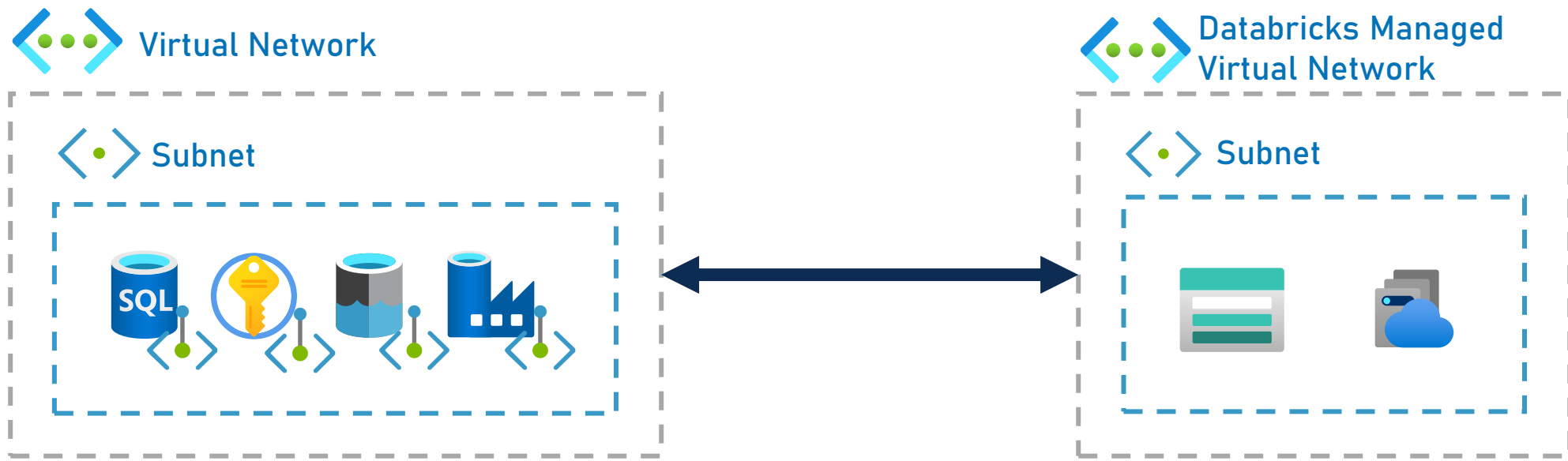


NOTE: Azure Private Link <> Azure Private Link [Service](#)

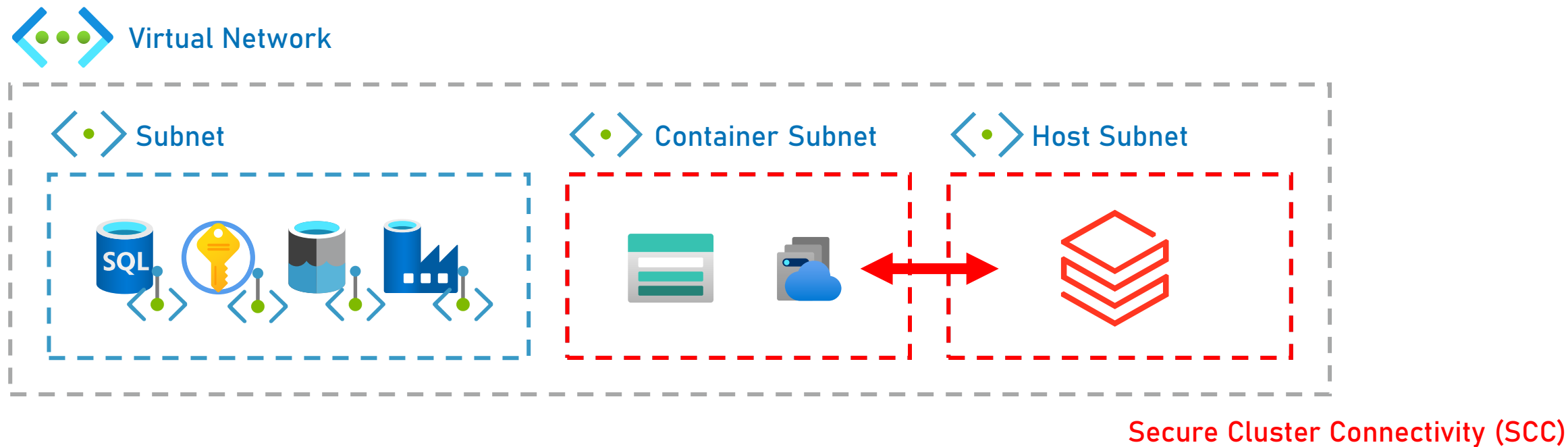
PRIVATE ENDPOINTS



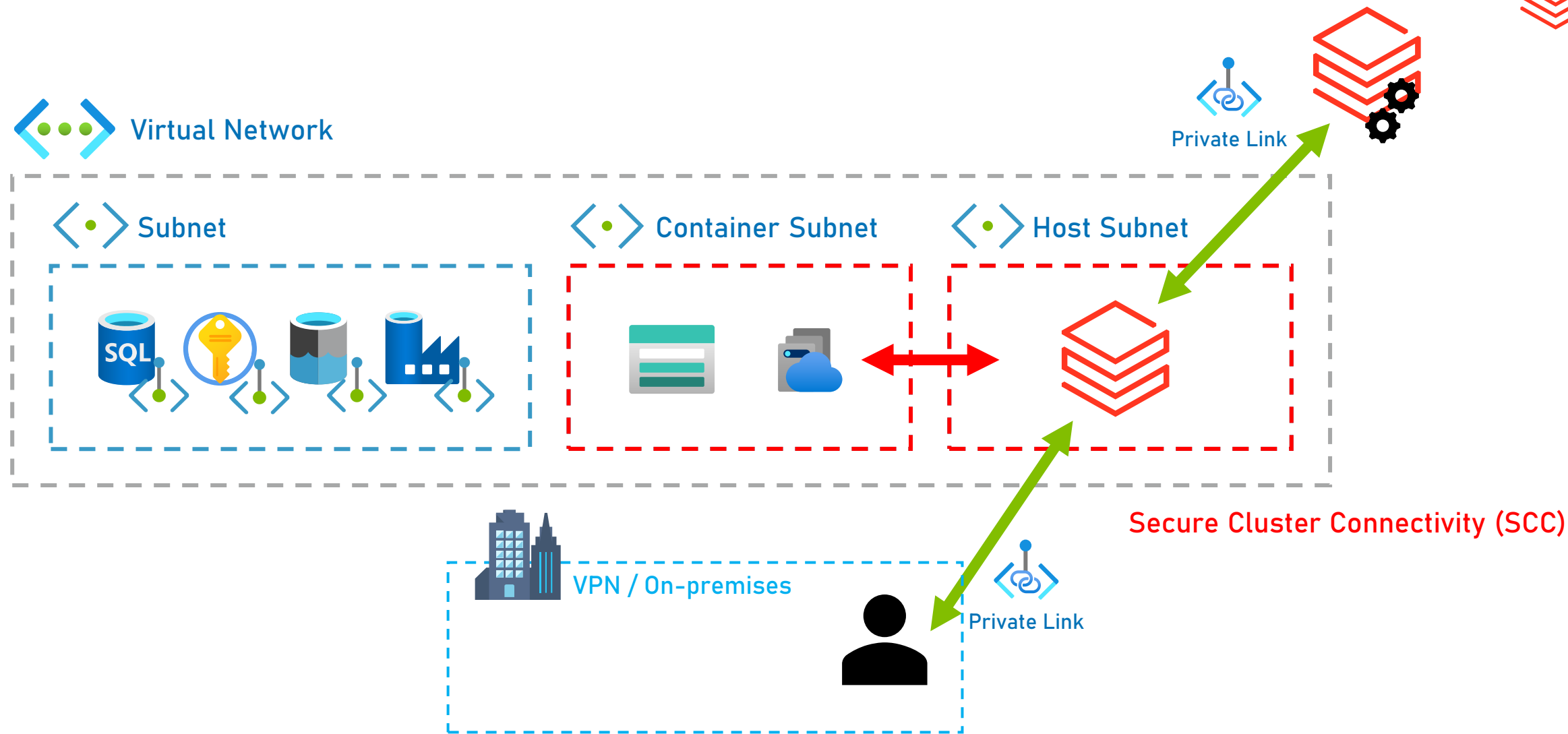
DATABRICKS VNET PEERING



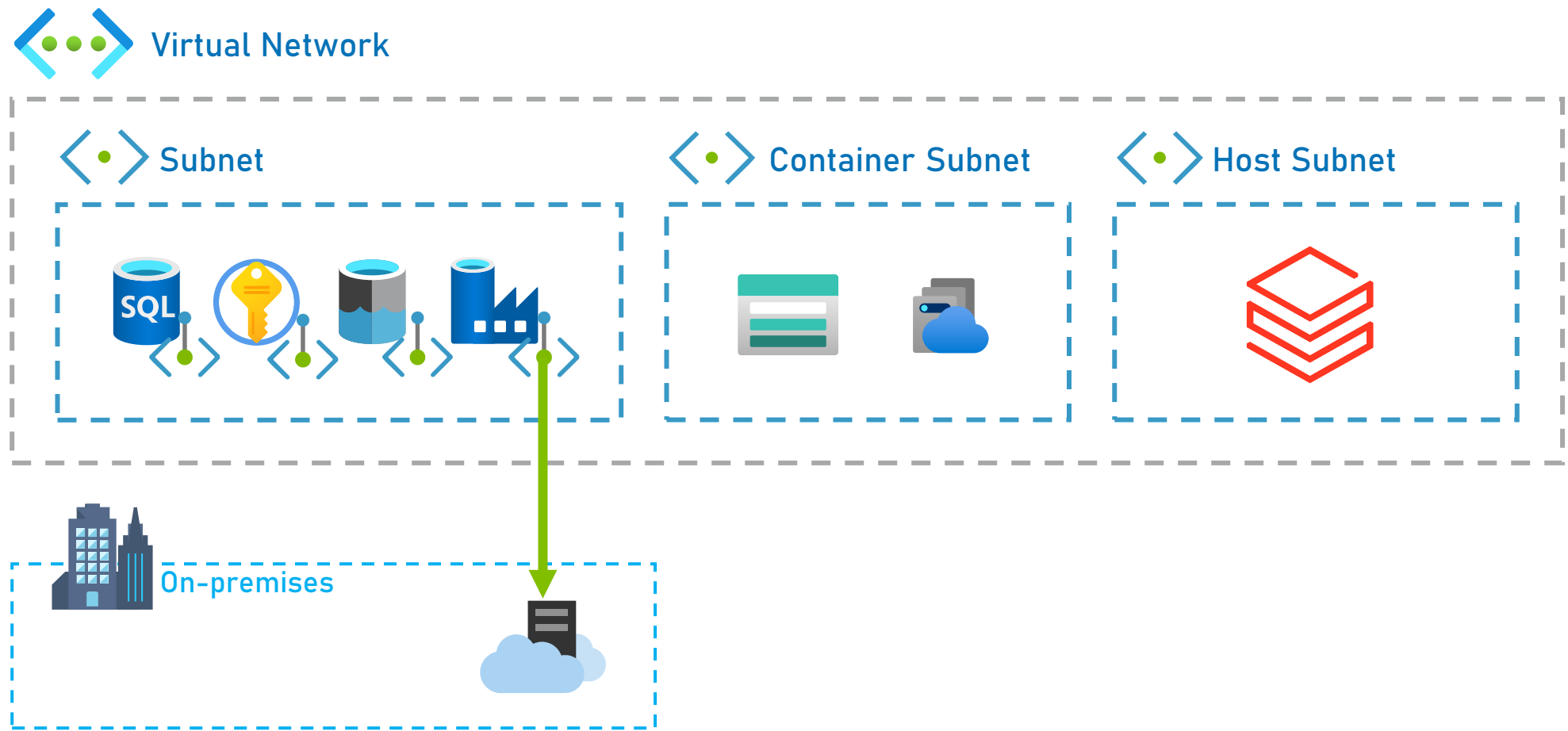
DATABRICKS VNET INJECTION

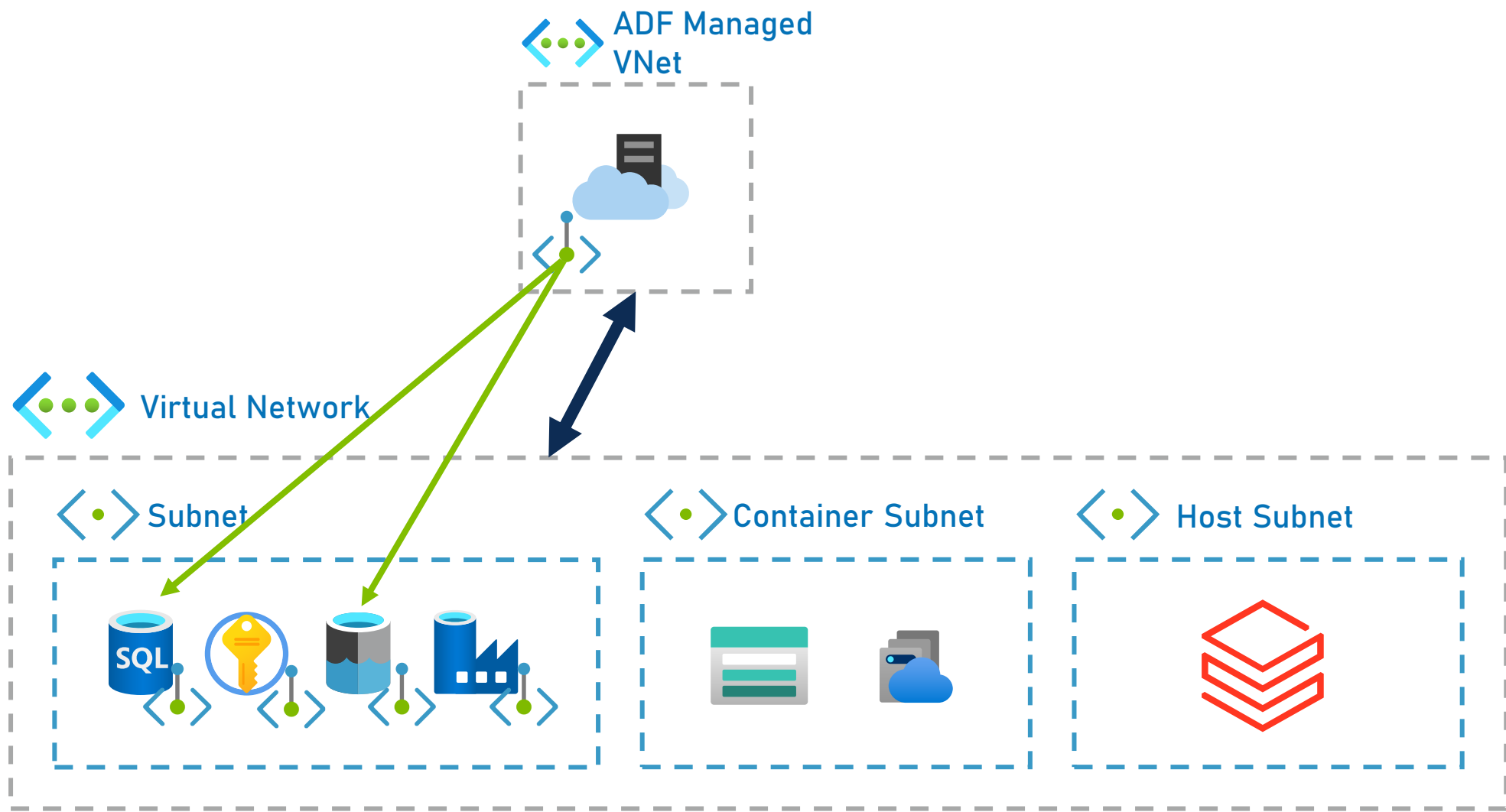


DATABRICKS VNET INJECTION

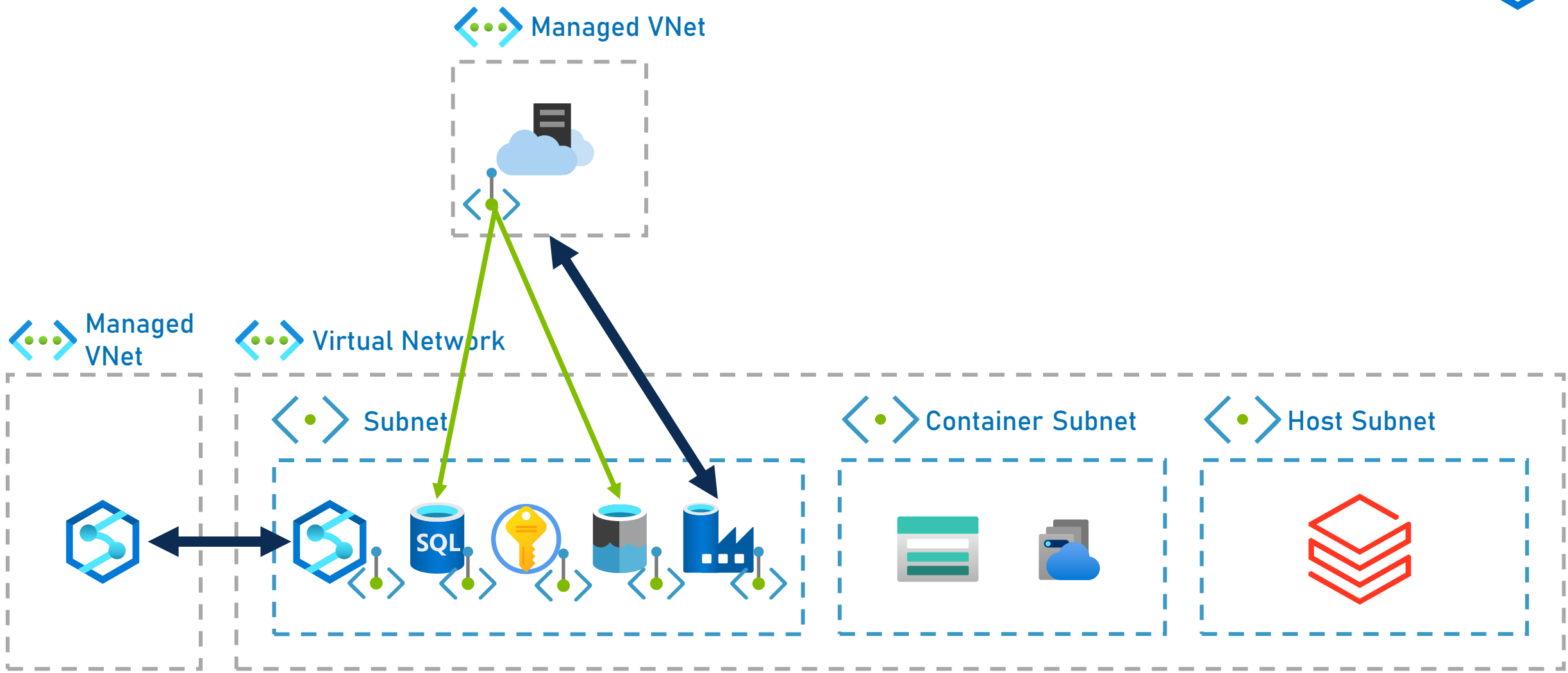


DATA FACTORY ON-PREMISES CONNECTIVITY

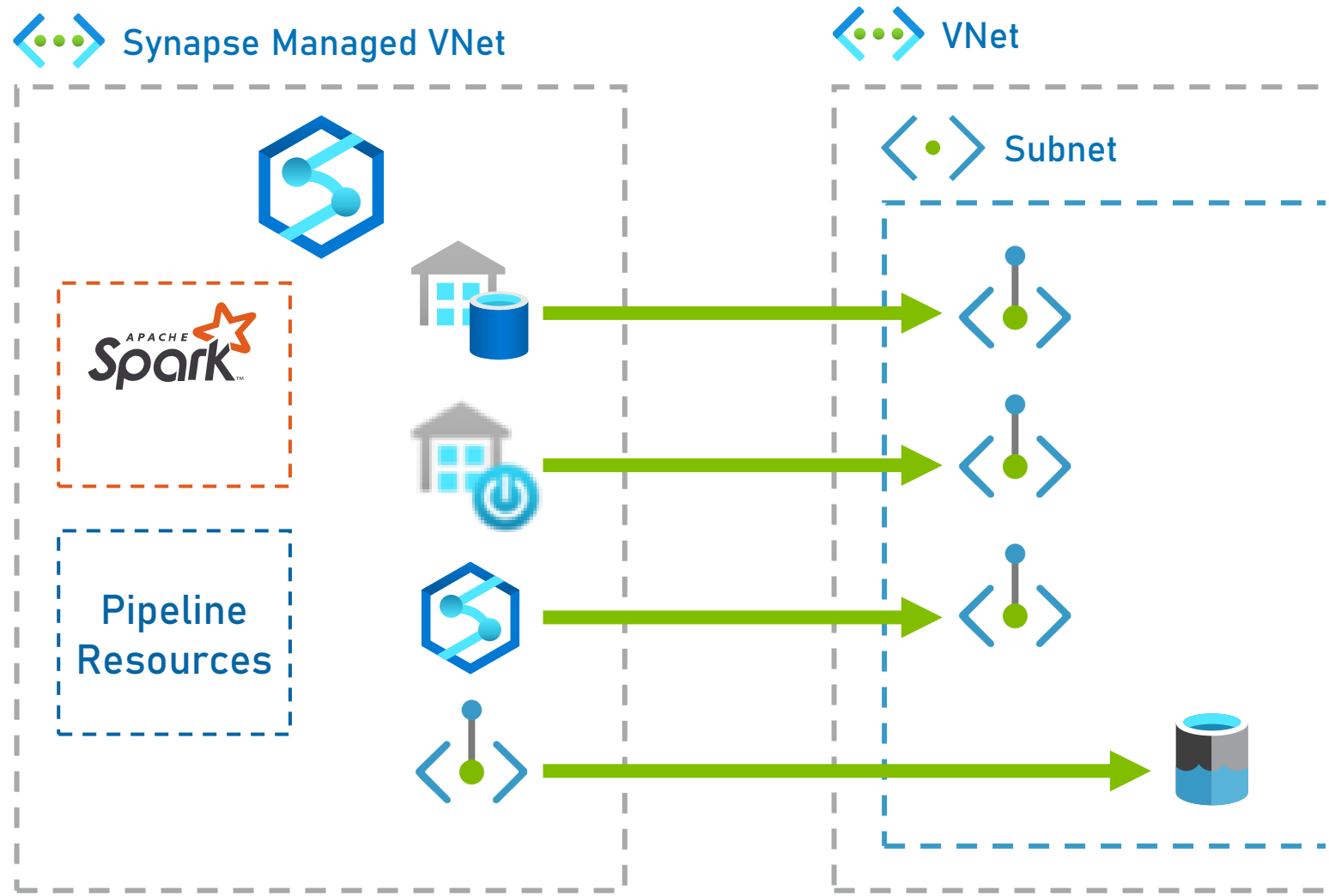




WHAT ABOUT AZURE SYNAPSE?



WHAT ABOUT AZURE SYNAPSE?



SUMMARY



Virtual Network (VNet)



Traffic is privately secured within the organisation



Integrate with existing securely networked resources via Hub > Spoke



Microsoft-hosted Azure DevOps Agent



Self-hosted (IaaS)



Connectivity restrictions



Azure Bastion/Jump box (IaaS)



Increased costs



Don't underestimate complexity (NSGs, DNS zones, etc)



www.advancinganalytics.co.uk

DATA & IDENTITY SECURITY



@ADVANCINGANALYTICS



@ADVANALYTICSUK



/ADVANCING ANALYTICS

SECURITY FEATURES



Microsoft
Managed
Keys

Secure
Cluster
Connectivity

Premium
Tier



Transparent
Data
Encryption

Azure SQL
Auditing



Microsoft
Managed
Keys

Managed
Identity

Managed
Vnet on IR

SHIR to use
Private
Endpoint



Microsoft
Managed
Keys

No
Anonymous
Access

Disable Blob
Public
Access



Azure
RBAC

Soft Delete

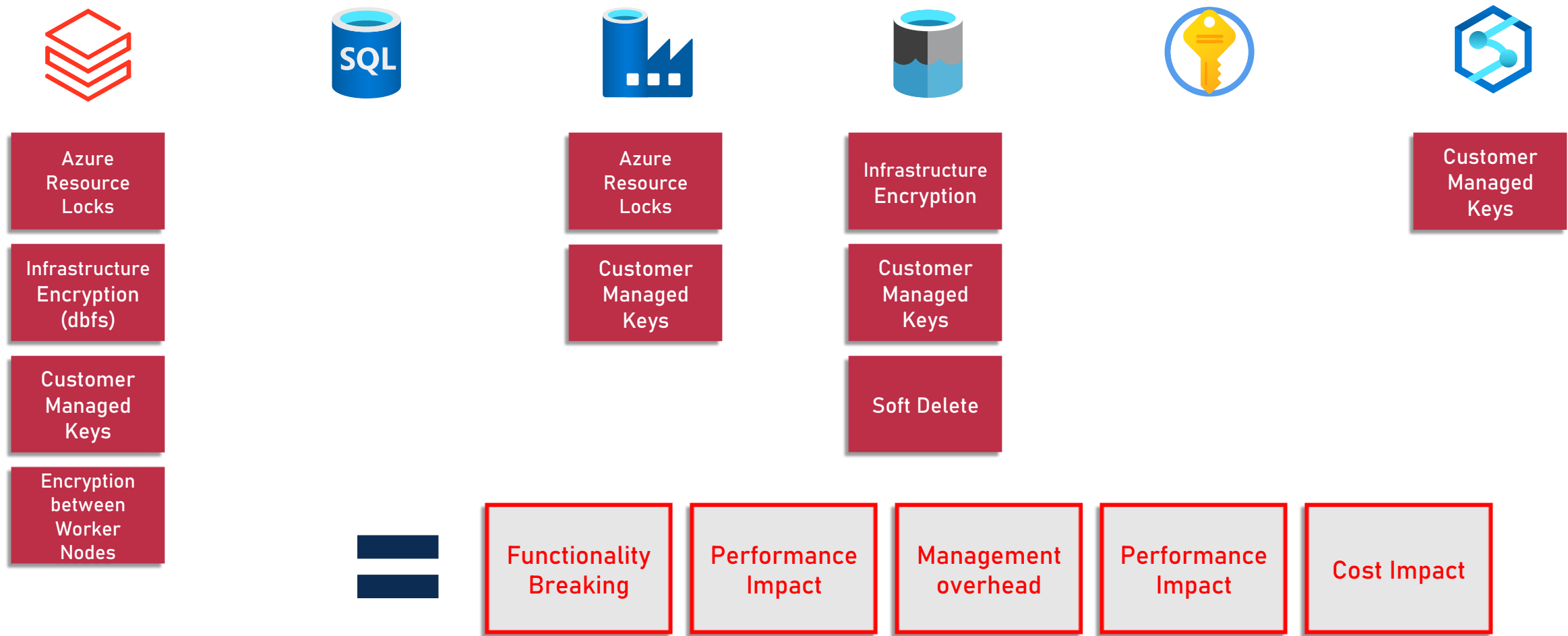


Microsoft
Managed
Keys

Azure SQL
Auditing

Managed
Vnet

USE WITH CAUTION



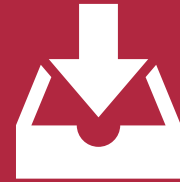
SUMMARY



Existing Azure
Policies



Some features
don't make
sense



Additional
support
overhead

INFOSEC WISH LIST



Azure
Sentinel



CIS
Benchmark



SUMMARY



Design for
Security



RBAC First



Defence in
Depth



Don't just turn
everything on



Don't
underestimate
complexity





THANK YOU



<https://craigporteous.com>



@cporteous



<https://github.com/cporteu>



@ADVANCINGANALYTICS



@ADVANALYTICSUK



/ADVANCING ANALYTICS

REFERENCES

- [How to protect Data Exfiltration with Azure Databricks to help ensure Cloud Security](#)
- [Deploy Azure Databricks in your Azure virtual network \(VNet injection\) - Azure Databricks | Microsoft Docs](#)
- [Secure cluster connectivity \(No Public IP / NPIP\) - Azure Databricks | Microsoft Docs](#)
- [Azure Synapse Analytics security white paper: Network security - Azure Synapse Analytics | Microsoft Docs](#)
- [The Purpose and Pain of Azure Resource Locks - Craig Porteous](#)
- [Mapping Data Personas to your Data Platform - Craig Porteous](#)

